IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF MISSISSIPPI

UNITED STATES OF AMERICA

VS. NO.: 3:21-CR-107-NBB-RP

JAMARR SMITH, et al.

REBUTTAL MEMORANDUM OF AUTHORITIES IN SUPPORT OF MOTION TO SUPPRESS

COMES NOW, the Defendant, Jamarr Smith, by and through the undersigned counsel, and files this rebuttal memorandum of authorities in support of his Motion to Suppress, would state unto the Court as follows:

I. INTRODUCTION

The Supreme Court has held that probable cause of issuance of a warrant must be particularized with respect to the specific person sought to be searched. Here, the government had no identifiable suspects at all as to the robbery of the Lake Cormorant Post Office, so it caused a warrant to be issued that searched 592 million Google accounts. Is that constitutional?

Assuming that the geofence warrant was unconstitutional (as other courts have found), does the good faith exception apply when the warrant application stated that a video of the incident showed that one of the suspects was "possibly using a cellular device," but the government now admits that no cell phone use was in fact shown at all?

II. DISCUSSION

The government makes four primary arguments in response to the defendant's motion:

1. The warrant satisfied the Fourth Amendment because there was probable cause and was particular (and embedded therein is the contention that the defendants herein lack standing to challenge the government's accessing location history of persons not suspected of a crime).

2. Even if the warrant was unconstitutional, the good faith exception applies.

3. The application and the warrant did not mean what it said about "further legal process."

4. The warrant did not constitute a search, and Smith had no expectation of privacy in his location history.

The defendant will address these arguments in order. The defendant will conclude with a brief discussion of reported cases involving geofence warrants to show that the only court to consider the issue with a full record found that such warrants are unconstitutional.

A. Probable cause and particularity.

As discussed in the original submission, "dragnet" searches are a perennial Fourth Amendment fear. That is why the Constitution prohibits general warrants and requires both probable cause and sufficient particularity. The warrant here failed the probable cause prong because the government did not request data from specific users or accounts; instead, it required Google to search 592 million accounts – a crucial fact the government does not address at all in its response. The warrant failed the particularity prong because it gave the government broad discretion over what information to obtain – the hallmark of a non-particular warrant.

1. The government does not address the undisputed fact that this warrant required the search of 592 million Google accounts.

Relying on *Illinois v. Gates*, 462 U.S. 213, 238 (1983), the government asserts that the probable cause prong is met in this case because "there was more than a fair probability that the suspects were within the geofence during the time period referenced in the warrant."[1] (Government's Response to Defendant's Motion to Suppress (hereinafter "Response"), p. 10).

[1] As will be discussed further below, the Court needs to immediately ask in response to this assertion: *Which* suspects? It is undisputed that the government had no suspects at all when it applied for the warrant.

The only district court to consider this question with a more complete factual record concerning the true breadth of searches required by geofence warrants, the United States District Court for the Eastern District of Virginia, categorically rejected the exact same arguments the government is making here. *United States v. Chatrie*, 590 F. Supp. 3d 901, 929–33 (E.D. Va. 2022) (stating "[T]he warrant simply did not include any facts to establish probable cause to collect such broad and intrusive data from each one of these individuals.").[2]

First, the Court should not be misdirected into believing that this warrant sought location history only for Jamarr Smith, Thomas Iroko Ayodele and Gilbert McThunel – or that there was a "fair probability that [these] suspects were within the geofence during the time period referenced in the warrant." These persons were not known to the government when the warrant was sought and issued, meaning the government could not have had probable cause to search their Google accounts. Instead, the warrant authorized the search of location history from hundreds of millions of Google accounts in an effort to identify potential suspects. So the idea that there was a "more than fair probability" that these three specific persons were within the geofence at relevant times is not correct.

Then, without conceding, disputing or even noting that its warrant required the search of 592 million Google accounts, the government contends that, well, even if it did not have probable cause to search these specific defendants' location history, it could use the information to identify witnesses and some generic "further evidence," or to corroborate and explain other evidence, or to rebut defenses asserted by the defendants that some other person was involved.

[2] The government suggests that the *Chatrie* decision was perhaps guided by District Judge Hannah Lauck's "personal opposition" to geofence warrants. (Response, p. 18). The defendants reply that it would probably be more fair and respectful of Judge Lauck's position to state that her decision was guided by a professional and judicial opposition to unconstitutional warrants.

(Response, pp. 11-12). The court in *Chatrie* rejected this, stating:

> Law enforcement attempted to justify the warrant by claiming that such a sweeping search "may [have] tend[ed] to identify potential witnesses and/or suspects.". . . Even if this Court were to assume that a warrant would be justified on the grounds that a search would yield witnesses (some of whom had already been interviewed) instead of perpetrators, the Geofence Warrant is completely devoid of any suggestion that all—or even a substantial number of—the individuals searched had participated in or witnessed the crime. To be sure, a fair probability may have existed that the Geofence Warrant would generate the suspect's location information. However, the warrant, on its face, also swept in unrestricted location data for private citizens who had no reason to incur Government scrutiny.

Id. at 929-30 (citations omitted).

In reality, as discussed in the initial submission, the government is just making the same argument that was rejected by the Supreme Court in *Ybarra v. Illinois* that, because the government thought a crime had been committed within the geofence, it had probable cause to search any and all Google accounts that might have had location history enabled within the fence. The court in *Chatrie* rejected this as "inverted probable cause" – "that law enforcement may seek information based on probable cause that some unknown person committed an offense, and therefore search every person present nearby." *Id.* at 933. Instead, *Ybarra* requires: "Where the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person." *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979); *see Chatrie*, 590 F. Supp. 3d at 933 (stating "the Government's argument rests on precisely the same 'mere propinquity to others' rationale the Supreme Court has already rejected as an appropriate basis for a warrant.") (citing *Ybarra*, 444 U.S. at 91).

In short, the warrant was profoundly overbroad. The government simply did not have probable cause to search 592 million Google accounts. It did not have probably cause to search

any of the accounts that Google initially identified. Indeed, it did not have probable cause to search even one account because the government had no identifiable suspects, much less a suspect that it believed was using Location History on his or her phone.

2. The warrant gave the government (and Google) broad discretion over what information to obtain in Steps 2 and 3 of the process.

The Court is well aware that a valid warrant must particularly describe the place to be searched and the items to be seized so that nothing is left to the discretion of the officer in executing the warrant. *Marron v. United States*, 275 U.S. 192, 196 (1927); *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). This warrant failed that requirement because, in Steps 2 and 3 of the process, after Google produced the anonymous information regarding devices in Step 1, the government decided what was "relevant" and then obtained de-anonymized information without returning to the court for an additional authorization (as the warrant stated it would do – which will be discussed further below).

As to the particularity requirement, the government focuses its response on the idea that Step 1 of the warrant process was limited to a one-hour interval for a specific date and location, and then the process was further narrowed down through Steps 2 and 3. The government does not address the fact that it was *the government* that decided which google users to search in Steps 2 and 3. Again, the court in *Chatrie* rejected these same arguments:

> To the extent the Government would attempt to argue in the alternative that this warrant's three-step process cures any defects with the warrant's particularized probable cause, such an argument is unavailing. Even if this narrowing process cured any of the warrant's shortcomings as to particularized probable cause, this process cannot independently buttress the warrant for an entirely separate reason: clear lack of particularity. Warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. In other words, "[a] warrant that meets the particularity requirement leaves the executing officer with no discretion as what to seize." But Steps 2

> and 3 of this warrant leave the executing officer with unbridled discretion and lack any semblance of objective criteria to guide how officers would narrow the lists of users.

Chatrie, 580 F. Supp. 3d 933-34 (citations omitted). Thus, this excessive governmental discretion in warrant-based searches renders this warrant unconstitutional.

3. Standing.

The government contends that the defendants' herein lack standing to challenge the government's acquisition of non-party location data. (Response, p. 12). To be clear, *the government* certainly contends that it searched Jamarr Smith's and Gilbert McThunel's location history. If the government is correct that it did so, then the government would have to concede that the defendants at least have standing to object to a search of their location history.

As discussed extensively above, the government had no probable cause whatsoever to search anybody's location history, much less the defendants', because it had no identifiable suspects.[3]

B. The good faith exception does not apply.

United States v. Leon sets out circumstances where the good faith exception does not apply, three of which are clearly applicable here:

1) the warrant is based on recklessly false statements;

2) the affidavit lacks substantial basis to determine probable cause; and

3) the warrant was facially deficient.

United States v. Leon, 468 U.S. 897, 914-15 (1984).

[3] Further, as will be discussed in the next section, the grossly overbroad scope of the search is relevant to the good faith analysis: Would the magistrate have approved the warrant if the application had properly disclosed that it required the search of 592 million Google accounts?

1. Recklessly false statements.

The warrant application contains this recklessly false statement: "Postal Inspectors conducted a detailed review of the video surveillance and it appears the robbery suspect is possibly using a cellular device both before and after the robbery occurs." (Exh. B, ¶ 16). Notably in its response, the government attempts to recast the facts underlying this representation by conceding that the video does not show the assailant "using a cellular device," but instead shows the assailant walking around with his left hand by his or her ear – and further conceding that no phone is shown on camera. (Response, p. 19). While the defendants absolutely deny that the video shows anything of the sort, this remarkable concession in fact confirms that the warrant application was recklessly false, or at a minimum "manipulated facts subtly," which is equally prohibited. *See United States v. Namer*, 680 F.2d 1088, 1093 n.10 (5th Cir. 1982). At any rate, this is clearly not a case of mere negligence in the representation – the agent knew the video did not show anybody using a phone, yet stated in his affidavit that the video showed "possible" cell phone use.

Another misrepresentation in the affidavit was the agent's omission of the true scope of the number of people to be searched and the true boundaries of the "geofence." Had the magistrate known that the warrant he signed authorized Google to search the private daily journals of 592 million people, surely he would have refused to sign such a warrant. To not include those facts demonstrates at least recklessness with regard to the true nature of the search the affiant proposed. The unprecedented search of hundreds of millions of private diaries at once also renders the warrant so overbroad that no reasonably objective officer would have thought it a valid warrant.

2. No substantial basis to determine probable cause.

The geofence warrant was "so lacking in indicia of probable cause" to search 592 million Google account holders that "official belief in its existence [was] entirely unreasonable." *See Leon*, 468 U.S. at 923. As discussed in the initial submission, the warrant application contained a bare-bones affidavit, defined as one that "contain[s] wholly conclusory statements, which lack the facts and circumstances from which a magistrate can independently determine probable cause." *United States v. Satterwhite*, 980 F.2d 317, 321 (5th Cir. 1992) (citation omitted). Simply stated, the affidavit in this case contained no information whatsoever that probable cause existed to search 592 million Google accounts in hopes that one or more of them would show up in the geofence.

3. The warrant was facially deficient.

The good faith exception should not apply because the geofence warrant was "facially deficient." *See Leon*, 468 U.S. at 923. It sought unfettered discretion to search deeply private data of an unlimited number of people, and was so lacking in probable cause and particularity that "the executing officers [could not have] reasonably presume[d] it to be valid." *Id.* As discussed above, the government does not even address the fact that this warrant caused Google to search 592 million user accounts – a fact that even the most inexperienced postal inspector would conclude is overbroad and improper.

C. The warrant meant what it said about further legal process.

The warrant application clearly stated that after Google provided anonymous information pursuant to Step 1, the government would undertake "further legal process" to obtain the de-anonymized information in Steps 2 and 3:

> [location data will] be provided by Google [which] will be identified only by a numerical identifier, without further content or

> information identifying the user of a particular device. Law enforcement will analyze this location data to identify users who may have witnessed or participated in the Subject Offenses and *will seek any additional information regarding those devices through further legal process.*

(Exh. B, ¶ 21b.). The government is correct that the defendants believe that this clear language required the government to return to the magistrate to obtain this information. (Response, p. 21). The government contends that, because the warrant stated what was to happen in Steps 2 and 3, it did not mean what it said, and the government did not have to obtain "further legal process" after all.

This is really not a legal question beyond the fact that the Court "must read the warrant as written." *United States v. Crandall*, 2012 WL 5430339, at *4 (D. Mont. Nov. 1, 2012); *see also United States v. Burch*, 432 F. Supp. 961, 963 (D. Del. 1977) (stating "the validity of a warrant must be tested by a court's interpretation of the warrant as written."). To have any meaning at all, "further legal process" must mean that some *additional* legal process that had not been undertaken to that point had to be undertaken in order to receive the de-anonymized information. Black's Law dictionary does not define "legal process," but it defines "legal proceedings" as "all proceedings authorized or sanctioned by law, and brought or instituted in a court or legal tribunal, for acquiring a right or the enforcement of a remedy." Black's Law Dictionary, 5th Ed.

The defendants' interpretation makes sense because the government had just undertaken a massive (unprecedented, really) search of hundreds of millions of Google accounts and, in a (misguided and ultimately unconstitutional) effort to protect the privacy of these account holders, received information that did not identify any particular person or account. As discussed above, Steps 2 and 3 granted the government excessive discretion in what de-anonymized accounts it wanted to have – and knowing that warrants must be particular and not leave the determination

of what the warrant seeks to the government,[4] the government knew it had to go back to the magistrate to receive this additional information. This it did not do.

D. The defendants had a reasonable expectation of privacy in their location history, and the government conducted a search.

1. Obtaining location data in this case was certainly a search.

The government contends that the defendants had no privacy interest in two hours of location information, arguing: (1) though *Carpenter v. United States*, 138 S. Ct. 2206 (2018) does not explicitly hold that obtaining two hours of location data is not a search, (2) the Court can extrapolate that it was not a search because such a short period of data is only 1/84th of the period of time (seven days) found constitutionally infirm in *Carpenter*; therefore, (3) the Court should create a *de minimis* exception to the Fourth Amendment.

First, the Court in *Carpenter* made it clear that it would not "grant the state unrestricted access to a wireless carrier's database of physical location information," describing such information as "deeply revealing," "comprehensive," and "inescapable." *Id.* at 2223. Google location history is way more revealing, comprehensive and inescapable than the cell site location information ("CSLI") at issue in *Carpenter*. In fact, CSLI is just one of the data sources that Google collects and uses to determine users' locations. But Google also includes GPS location data as well as "additional information from nearby Wi-Fi, mobile networks, and device sensors." Google Policies, Location Data (Nov. 20, 2018), https://policies.google.com/technologies/location-data?hl=en. Indeed, Google uses it for that very purpose when selling advertisements. *Id.* As a result, Google location information is significantly more precise (and potent) than CSLI alone. Specifically, a single data point from CSLI may only be capable of revealing a neighborhood or zip code that a device is in. Google

[4] *Marron*, 275 U.S. at 196; *Coolidge*, 403 U.S. at 467.

location history can pinpoint a device's location inside a house or a church.

The defendants' had a reasonable expectation of privacy in their Google location information because it was at least as private as the records in *Carpenter*. That case involved two orders for CSLI: one seeking 152 days, and a second for seven days. *Id.* at 2212. In holding that a warrant is required for seven days or more of CSLI, the Court merely decided *Carpenter* on the facts before it. There is no higher constitutional significance to seven days, and *Carpenter* does not suggest that the Fourth Amendment would condone warrantless searches for a shorter period of time. In fact, the second CSLI order only produced only two days of records, not seven. *Id.* While some physical searches may be permissible without a warrant, the Court has been clear that "any extension of that reasoning to digital data has to rest on its own bottom." *Riley v. California*, 134 S. Ct. 2473, 2489 (2014).

The fact that the government obtained a smaller quantity of this location data than in *Carpenter* does not diminish its potentially revealing nature. *Carpenter* emphasized the long-term privacy implications of cell phone location tracking only because those were the facts before the Court. Elsewhere, the Justices have expressed concern with even short-term monitoring. In *United States v. Karo*, for example, the use of a beeper to track a drum of ether inside a private residence was sufficient to trigger Fourth Amendment scrutiny. *United States v. Karo*, 468 U.S. 705, 716 (1984) ("We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device . . . whether a particular article—or a person, for that matter—is in an individual's home at a particular time."). Just a small window of GPS monitoring still creates a "precise, comprehensive record of a person's movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *United States v. Jones*,

565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). Indeed, it takes little imagination to conjure the privacy implications of even a single trip to "the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Id.* (quoting *People v. Weaver*, 12 N.Y.3d 433, 441-442 (2009)).

2. The Third-Party doctrine does not apply.

The third-party doctrine generally holds that individuals do not have a reasonable expectation of privacy in information "voluntarily" conveyed to a third-party, but the *Carpenter* Court was clear that the rule is not to be "mechanically" applied in the digital age. *Carpenter*, 138 S. Ct. at 2219. Instead, *Carpenter* teaches that mobile location information is a "qualitatively different category" of data, distinct from the telephone numbers and bank records in *United States v. Miller*, 425 U.S. 435 (1976), or *Smith v. Maryland*, 442 U.S. 735 (1979). *Id.* at 2216–17. Location history "gives police access to a category of information otherwise unknowable." *Id.* at 2218.

The court in *Chatrie* stated:

> But the Court remains unconvinced that the third-party doctrine would render hollow Chatrie's expectation of privacy in his data, even for "just" two hours. Google Location History information—perhaps even more so than the cell-site location information at issue in *Carpenter*—is "detailed, encyclopedic, and effortlessly compiled." *Carpenter*, 138 S. Ct. at 2216; see id. at 2219 ("There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today."). Although, unlike in *Carpenter*, Chatrie apparently took some affirmative steps to enable location history, those steps likely do not constitute a full assumption of the attendant risk of permanently disclosing one's whereabouts during almost every minute of every hour of every day.

Chatrie, 590 F. Supp. 3d at 935–36. The Court should apply the same reasoning here and reject

the government's third-party argument.

E. A brief note about other reported cases involving geofence warrants.

The government helpfully lists six reported cases involving geofence warrants, five by magistrate judges and one by a district judge, which is *Chatrie*. Using the government's short-hand, the magistrate judge decisions are: 2020 WL 5491763 (E.D. Ill. 2020) (Google I), 481 F. Supp. 3d 730 (E.D. Ill. 2020) (Google II), 497 F. Supp. 3d 345 (E.D. Ill. 2020) (Google III), and 542 F. Supp. 3d 1153 (D. Kan. 2021) (Google IV), 579 F. Supp. 3d 62 (D. D.C. 2021) (Google V). Two of the cases granted the geofence warrants, three of them denied the warrants. While much of the analysis in these magistrate judge decisions is certainly helpful, the Court should note that these were *ex parte* decisions not contested by a defendant, and none had the highly developed record present in *Chatrie* and this case. Therefore, *Chatrie* should carry significantly more precedential weight, and the defendants would again state that the Court in *Chatrie* addressed and rejected most of the arguments presented by the government in this case.[5]

III. CONCLUSION

Based upon the forgoing, the Court should suppress the evidence that the government obtained pursuant to the warrant to Google at issue, as well as any other evidence derived from that information as fruit of the poisonous tree. Jamarr Smith requests any further relief the Court may find warranted in the premises.

[5] In fairness, there is another case involving a motion to suppress a geofence warrant that was contested: *United States v. Davis*, 2022 WL 3009240 (M.D. Ala. July 1, 2022), report and recommendation of magistrate accepted by district court, *United States v. Davis*, 2022 WL 3007744 (M.D. Ala. July 28, 2022). Though this case post-dates *Chatrie*, that decision is barely discussed, and only to state that the court therein found the good faith exception applied. Further, there is no indication that the Davis court had the record concerning the scope of the search (592 million Google accounts) before it. Though the court denied the motion to suppress, it did so on the issue of standing and found the good faith exception applies. Of course, the good faith exception is highly fact-specific, and *Davis* would not be instructive on that issue here.

RESPECTFULLY SUBMITTED,

JAMARR SMITH

HICKMAN, GOZA & SPRAGINS, PLLC
Attorneys at Law
Post Office Drawer 668
Oxford, MS 38655-0668
(662) 234-4000 telephone
(662) 234-2000 facsimile
glewis@hickmanlaw.com

BY: */s/ Goodloe T. Lewis*
GOODLOE T. LEWIS, MSB # 9889

CERTIFICATE OF SERVICE

I, GOODLOE T. LEWIS, attorney for JAMARR SMITH, do hereby certify that I have on this date electronically filed the foregoing document with the Clerk of Court using the ECF system which sent notification of such filing to all counsel of record, including:

Robert Mims
Office of the US Attorney
900 Jefferson Avenue
Oxford, MS 38655
rmims@usadoj.gov

DATED: December 9, 2022.

/s/ Goodloe T. Lewis
GOODLOE T. LEWIS

GOODLOE T. LEWIS, MSB # 9889
HICKMAN, GOZA & SPRAGINS, PLLC
Attorneys at Law
Post Office Drawer 668
Oxford, MS 38655-0668